BY ORDER OF THE COMMANDER
AIR FORCE SPECIAL OPERATIONS COMMAND

AFSOC INSTRUCTION 33-201
15 March 1998

Communications

AFSOC COMPUTER SECURITY FOR INFORMATION SYSTEMS (Networks) PROCESSING AT THE SENSITIVE UNCLASSIFIED (SU) LEVEL

COMPLIANCE WITH THIS INSTRUCTION IS MANDATORY. This instruction implements Air Force Policy Directive (AFPD) 33-2*, Information Protection*; DoD 5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (the "Orange Book"); and NCSC-TG-005 Version 1, Trusted Network Interpretation (TNI), also known as the "Red Book," to the operational requirements of the network. This instruction pertains to all AFSOC and AFSOC-gained units.

SUMMARY OF REVISIONS

This revision changes the terms Automated Information System (AIS) to Information System (IS), Sensitive But Unclassified (SBU) to Sensitive Unclassified (SU), and EMISSION SECURITY to EMSEC. It deletes the term INFOSEC; updates the references from AFSSM 5007 to AFMAN 33-229, AFI 33-202 to AFSSI 5024 Vol I, AFSSM 5018 to AFSSI 5024 Vol II; changes the password length to eight characters and requires special characters and/or numbers; requires the CSO/SA to ensure the user completes the required SATE training prior to logging on; requires the unit CSOs to maintain and provide the Wing Information Protection Office an updated list of workstations with modems showing justification for modem use, location of workstation, user, and modem number; addresses compact discs as storage media; and updates the banner required on all information systems.

Supersedes AFSOC Instruction 33-201, 1 August 1995
OPR: HQ AFSOC/SCMS (Mr. Frank Zoldak)
Certified by: HQ AFSOC/SCM (Maj Oliver Bryant)
Pages: 15
Distribution: F

1. Introduction:

1.1. Purpose. The purpose of this document is to establish operational security instructions for Information Systems (network) processing information at the sensitive unclassified (SU) level. It details how the risk of operating a network will be minimized by coordinated implementation of specialized disciplines of personnel security, physical security, operations security (OPSEC), computer security (COMPUSEC), information security, communications security (COMSEC), emanations security (EMSEC), and Fraud, Waste, and Abuse (FWA). It also specifies minimum security measures for systems or networks interfacing with the network.

1.2. Applicability and Scope. This security instruction shall put into effect the set of laws, rules, and practices regulating management, protection, and distribution of data entrusted to a network. It is written for security personnel of an operational wing-level system, or a major command (MAJCOM) system. Whenever this instruction refers to a network and it's Computer Security Officer (CSO) or Designated Approving Authority (DAA), it refers to a single system and the CSO (and alternates) or DAA associated with and responsible for that particular system, unless otherwise specified. This instruction shall apply to system users and personnel who maintain and administer a network. This instruction does not replace security requirements or regulations of higher organizational levels. This instruction will not be changed without MAJCOM DAA approval. Conflict between requirements interpretation in this policy and higher level requirements shall be brought to the attention of the network security office. When conflict exists, the CSO shall enforce the more stringent interpretation until the area of conflict is resolved and the recommended action is documented and approved.

1.3. Terms. Terms used in this document can be found in AFI 33-270, C4 Systems Security Glossary. A copy of this AFI shall be made available, by the Computer Security Officer, for continual reference. When necessary, terms in this instruction will be briefly explained for expediency.

1.4. Security Policy Objectives. This instruction has been written to satisfy specific security goals in a reasonable, pragmatic manner, with an eye toward future uses of a network. The instruction consolidates objectives found in DoDD 5200.28 and AFPD 33-2 with operational initiatives. The combined objectives are grouped into two categories: data processing, handling and storage; and system management.

1.4.1. Security Objectives for Data Processing, Handling, and Storage:

1.4.1.1. Confidentiality. Only personnel with proper authorization and need-to-know will be allowed access to data processed, handled, or stored on network components.

1.4.1.2. Integrity. Hardware and software resources of the system shall operate according to requirements and design documents. Unauthorized personnel will not be able to maliciously or unintentionally alter data processed, stored, or handled by the network and the data shall be accurate.

1.4.2. Additional Security Objectives Levied by System Management:

1.4.2.1. Mission Effectiveness. The network will ensure work can be accomplished in a timely manner with the degree of security assurance required by the mission. Disabling required computer security functions is not an acceptable method to achieve operational performance goals. If the impact is assessed to be beyond acceptable limits, users will formally submit to the DAA those features they require disabled. The DAA will be the approval authority for these requests.

1.4.2.2. User Acceptance. Computer security is an integral system component that enhances the operational environment by allowing the system, rather than the individual user, to manage system security. A network design goal is to ensure security mechanisms are useful tools and viewed as an ally, instead of an adversary, by the people who use it to accomplish their missions.

1.4.2.3. Economy. The network shall reflect sound fiscal management practices. Security mechanisms incorporated will be well founded, installed to perform in the most effective manner, and represent the best investment of each security dollar allocated. An economic analysis will be conducted to establish countermeasures to security holes. The DAA will review the economic analysis results and decide if the countermeasures are cost effective.

2. Mission. A mission statement for each network will be placed in an annex to this security policy by the NCC security manager.

3. Concept of Operations. A concept of operations statement for each network will be annotated in a supplement to this security policy.

4. Basic System Facts:

4.1. Classification of Information Processed. Data processed on the network will be no higher than sensitive unclassified.

4.2. Categories of Information Processed. No **formal** categories of sensitive unclassified information exist, however, some types of information with special handling and access instructions processed on an network (specifically For Official Use Only (FOUO) and Privacy Act (PA) information) have some of the characteristics of compartments that require extra protection. The addition of formal categories of information requiring an increased need for protection and access restriction will require a new risk analysis, certification, and DAA accreditation.

4.3. Minimum and Maximum User Clearances. Although sensitive unclassified information does not require a formal clearance, only individuals authorized by the DAA or designated representative will be allowed access to the network data.

4.4. Basic System Description:

4.4.1. System Assets. System assets and their configuration are identified in the network security architecture.

4.4.2. Physical, Logical, and Operational Aspects. Physical, logical, and operational aspects are identified in the network security architecture.

4.4.3. User Interactions With the System and Other System Interfaces. User interactions with the system and other system interfaces are identified in the network security architecture.

4.4.4. Intended System Capabilities and Functions. Intended system capabilities and functions are identified in the network security architecture.

4.4.5. Security Mode of Operations. All sensitive unclassified (SU) networks shall operate in the system high mode of operation.

4.4.6. Criticality Determination. A criticality determination for each network will be annotated in an annex to this security policy.

5. Roles and Responsibilities. Roles and responsibilities for security personnel are detailed in AFI 33-202, The Air Force Computer Security (COMPUSEC) Program. AFI 33-202 identifies security-related positions that must be filled. Because of personnel constraints, it is reasonable to task individuals to fill more than one position. Even though positions are combined, the responsibilities identified in AFI 33-202 still apply. The position titles and general duties of personnel at operational sites tasked with computer security responsibilities are summarized below. The network Certification and Accreditation Plan specifies the roles of all security personnel and clarifies the relationship between the organizational DAAs and the base level DAAs.

5.1. Designated Approving Authority (DAA). This individual is responsible for reviewing the computer security manager's certification package and site-specific implementation information to determine whether the networks' security provides the level of assurance required for operational use. The DAA shall also be responsible for the authorization of connection of systems to the network.

5.2. Base C4 Systems Security Office (BCSSO). This office shall administer the base computer security program. The office shall provide advice and guidance to computer security personnel and serve as an accreditation and connection approval advisor to local DAAs

5.3. Computer Systems Manager (CSM). The CSM is the individual administratively and operationally responsible for the computer system. The CSM shall supervise security personnel and manage IS components. The CSM shall have centralized responsibility for the maintenance and operational use, establishment and enforcement of the computer security policy. In this capacity, the CSM will certify to the DAA local security requirements have been met and the system meets the intent of the certification officials requirements. The CSM will also conduct additional testing of the system if there are differences in the environment of system configuration from that specified in the IS certification package. The CSM is responsible for overseeing the new risk analysis and certification actions and will provide the DAA a recommendation for or against accreditation and operational limitations. The CSM will also ensure any security deficiencies are documented in the complete accreditation package submitted to the DAA.

5.4. Computer Security Officer (CSO). The CSM shall appoint the CSO to provide day-to-day security administration. The CSO monitors activities at the facility and ensures compliance with higher level security regulations and guidance as well as local procedures. The CSO also performs initial evaluations of security problems, conducts security training, reviews proposed configuration changes for impact on security posture, and documents and reports security vulnerabilities and incidents. The CSO will have at least one fully trained alternate appointed at all times to preclude security and operational impacts during periods of TDY, sickness, and leave. The CSO and alternates shall perform the security software administration functions of the system as described in the Trusted Facilities Manual.

5.5. Unit Computer Security Officers (UCSOs). UCSOs will be appointed by the office chief or functional OPR of their workcenters to the CSO and will assist in directing the computer security program for terminal areas and remote terminals that are part of the IS. Each UCSO will ensure established security procedures are followed, report security vulnerabilities, incidents, and problems to the CSO, and ensure all users in their terminal area receive initial and recurring computer security training.

5.6. Users. Users are personnel able to log on the LAN. They are operational users, administrators, and maintainers of the LAN and components. All users shall comply with security policies and procedures and will report security problems to their respective UCSOs.

6. System Security Policy. The IS shall implement controlled access protection (CAP) functionality, as described in AFMAN 33-229, Controlled Access Program.

6.1 Operational:

6.1.1. Accountability:

6.1.1.1. Events and Information to be Audited**.** System audit records shall include:

6.1.1.1.1. Use of identification and authentication mechanisms, including successful and failed attempts to access the LAN and the reason for a failed attempt.

6.1.1.1.2. Successful and failed attempts to access selected protected objects (directories, files, programs, databases, etc). Starting and ending times of each access event shall be recorded using local or global synchronized time.

6.1.1.1.3. Deletion of selected objects, such as directories and files.

6.1.1.1.4 . Introduction of selected objects, such as executable programs, databases, and files into a user's address space

6.1.1.1.5. Use of all privileged, supervisory, or system-level commands and instructions capable of circumventing established security controls.

6.1.1.1.6. System restarts shall not record passwords or character strings incorrectly given as passwords which might possibly expose the password in the audit trail.

6.1.1.2 . Automated or Manual Audit. The CSO/SA may use a combination of automated and/or manual auditing techniques to perform an analysis of the collected audit data. As much as possible, the system shall automatically collect, process, and store security-relevant events which meet audit requirements. The CSO/SA shall be able to access the audit file immediately for real-time monitoring of the system. The system shall generate automated audit reports which will be available to the CSO/SA daily. The automated audit reports shall reflect those events which are indicative of malicious activity and shall include, at a minimum:

6.1.1.2.1. All access attempts. Many consecutive failed attempts by the same user or failed attempts by a vendor-defined default user are all indicators of a malicious user.

6.1.1.2.2. All unsuccessful attempts to access a file, program, database, or directory, especially the audit and security files.

6.1.1.2.3. Successful and unsuccessful use of all security-related commands.

6.1.1.2.4. The CSO/SA will review these audit reports daily, investigate and act immediately upon discrepancies and violations noted during the review.

6.1.1.3. Protection of Audit Files. The system shall limit access to audit information to only the CSO/SA or alternates. The system shall protect audit trail files in on-line storage from unauthorized changes, viewing, or destruction. The CSO/SA shall protect archived audit trail files stored on removable media in a safe location. Archived audit trail files shall be retained for a minimum of 6 months.

6.1.2. Access Control:

6.1.2.1. Method of Access Control. A combination of physical, personnel, and system security mechanisms shall control access to IS components. This section focuses on the system security mechanisms and later sections address the physical and personnel aspects of access. Two types of system security mechanisms apply to access control: initial system identification and access controls (logging on to the system) and system defined resource access controls (such as discretionary access control (DAC) access tables).

6.1.2.1.1. The system shall use the combination of a user identification (userID) for an individual user and a password known only to that user to control initial system access. The CSO/SA shall not allow the use of group IDs and passwords for initial system access. The CSO/SA shall change, as soon as safely possible, vendor-provided default passwords shipped with all IS components but not later than 30 days after installation. The user should also protect against tampering with the IS and information on unattended ISs. Provide protection by controlling physical access to the IS itself; by installing keyboard locks, BIOS passwords, password protected screen savers, etc.; or by establishing controls for removal and secure storage of information from unattended ISs.

6.1.2.1.2. Discretionary Access Control (DAC) is the mechanism by which users, either individual or group, are limited to the objects they may access. The principle of least privilege for access to system-defined resources will be utilized. This is the principle that a user should be given the least amount of power or privilege that still enables the individual to do his or her job. The system shall allow the CSO to define administrative groups of users with like resource access permissions and authority requirements for ease of security administration. If a user obtains access to a resource or performs a function as the result of a group permission or authority, the system shall identify in the audit trail the userID performing the action in addition to the group permission or authority on which the decision is based.

6.1.2.2. Password Length. Passwords which allow access to SU ISs must use eight characters (use upper and lower case) with at least one special character (@&+,etc.) and/or number. The IS system shall protect passwords and automatically perform password administration such that only the user has knowledge of their own password. Personnel shall apply a DAA-approved alternative means of positive identification to components which lack password capabilities.

6.1.2.3. Password Generation. Users shall generate their own personal passwords which conform to an operating system-controlled mask. The system shall not allow a new password which duplicates the old password nor shall it allow the new password to be the same as or a variation of the user-ID or the user's name. Variations are simple modifications to the user-ID or user name such as reversing the order of characters or adding a one digit prefix or suffix (OLDUSER becomes OLDUSER1, for example). Passwords shall be valid for no more than 90 days. The system shall prompt the user for a password change prior to expiration.

6.1.2.4. Password Destruction. The CSO/SA shall clear or destroy materials which contain expired passwords, such as paper or diskettes which contain active passwords. The CSO/SA shall clear reusable magnetic media according to DAA approved clearing procedures. The CSO/SA shall destroy materials which cannot be cleared or reused according to local destruction procedures.

6.1.2.5. Password Protection. The system shall protect password files so that users cannot access them (except to allow a user to change their personal password). All users shall protect their passwords as FOUO. Users shall not write down passwords (unless they are locked in a safe) or reveal them to anyone else, including the CSO. Only the system administrators shall have deletion rights to password files.

6.1.2.6. Changing Passwords. Users shall be able to change their own password anytime but no later than every 90 days.

6.1.2.6.1. The system administrators (SA) shall have the capability to immediately expire or invalidate user passwords. The system shall deny access to an expired password. To regain access privileges, the System Administrators must reactivate the user's account. The system administrator shall require the user to enter a new password to maintain password confidentiality.

6.1.2.6.2. Situations that require a CSO to expire a password immediately are when compromise of a user's password is suspected or known; when someone in the user's chain of command has identified an individual as a "disgruntled employee", when a UCSO notifies the CSO that an individual having knowledge of a password is transferred, discharged, or reassigned; or when an individual's commander denies that person access to the IS information.

6.1.2.7. Password Lockouts. The IS shall limit the number of consecutive incorrect access attempts by a userID to no more than three and shall automatically deactivate the userID after the third unsuccessful logon attempt. The system's action to deactivate a userID shall affect only that userID and shall not disable or otherwise affect the terminal or a different user who attempts to use the terminal. In recording the number of consecutive unsuccessful attempts for a specific userID prior to reaching the lockout threshold, the system shall reset the number to zero only after a successful login. For example, if a user has unsuccessfully tried to logon two consecutive times, he or she cannot reset the counter by either physically or logically disconnecting the terminal. The count may only be reset before the lockout threshold is met by logging on successfully.

6.1.2.8. Password Disclosure. Users shall not disclose their password to anyone. Users shall be responsible for actions attributed to the misuse of their password. If a user feels their password has been disclosed to another individual, they shall change it immediately and notify their CSSO or the CSO.

6.1.2.9. Systems Manager or User Privileges. Users with special permissions or privileges shall use them only for the requested or intended purpose. The CSO shall remove the permissions or privileges from those who abuse them. The CSO shall reinstate user privileges only upon the CSM's determination. The CSO/SA shall be the only users allowed to grant permissions or privileges.

6.1.2.10. Password Manager Requirements. The CSO/SA shall be the password manager. When a user account is newly created, the CSO/SA will either deactivate the account (the preferred method) or change the password to a random string. Deactivating the account is preferred because this allows the account to remain on the system, but in a completely unusable state. The CSO/SA shall not use default passwords and shall not write the password down. Before the user logs on the first time, the CSO/SA shall ensure the user completes the required SATE training and brief the importance of protecting passwords and choosing good passwords. After the initial password briefing is given, the CSO/SA shall reactivate the account or change the password. At the first login, the user shall enter a new password.

6.1.2.11. Dial-up and Remote Login Access. The CSM shall grant IS dial-up or other remote login access on a case-by-case basis and only after stringent review to determine the necessity for this kind of access. Remote users shall perform all logins, whether through a packet switched long-haul communications network or via modems, to a personal userID and password which conforms to the same rules as local users. The CSO shall not allow use of "guest" or "anonymous" accounts.

6.1.2.11.1. The CSO/SA shall create remote user accounts only upon CSM approval, providing the minimum requirements are satisfied.

6.1.2.11.2 . The requesting organization shall provide to the IS CSM sufficient information, such as a copy of the distant ends approval to operate letter, to ascertain the security environment at the distant end. The requesting organization shall define the scope and authority of interaction with the IS resources. The authority may be prescribed by military or contractual requirements. The requesting organization shall agree to abide by the policies in this document.

6.1.2.11.3. If user access is via modem and an automated security access mechanism is not available or implemented on the modem (such as caller authentication or automatic call-back), unattended access shall not be allowed.

6.1.2.11.4. Unit CSOs will maintain and provide the Wing Information Protection Office an updated list of workstations with modems showing justification for modem use, location of workstation, user, and modem number. Modem numbers will be released only to individuals with verified authorization. All personnel will protect modem numbers as “For Official Use Only”.

6.1.2.12. Time-out. The IS shall generate automatic time-outs for connected systems when inactivity exceeds 10 minutes. The CSO/SA may modify time limits on a case-by-case basis when operational usage patterns dictate. The system shall warn the user prior to system disconnection. Time-outs do not lock out the user from the system, the user need only login to the system again.

6.1.3. Personnel Security:

6.1.3.1. Security Clearances. Although no security clearance levels are required for SU information, a minimum of a favorable investigation (has a need-to-know) for all authorized users is required.

6.1.3.2. Need-to-Know. Personnel with system access must have a verified need-to-know for all data they can access. The CSO shall make the need-to-know determination based upon an access request by the user’s supervisor.

6.1.3.3. Situations Which Merit Denying Access. The CSO shall immediately deny or remove a user’s access if the user’s organization removes access for cause. The CSO shall, within 3 workdays, remove accounts of users who no longer require access in performance of their duties, have a permanent change of station, or have retired. A user’s organization will notify the CSO if a user will not require access for a period of 30 days or more; the CSO shall inactivate these accounts, and shall remove user accounts from the system if they have been inactive for a period of 180 days or more without prior coordination.

6.1.4. Physical Security. All personnel shall protect IS resources (processors, terminals, communications media) from natural threats (e.g., flood, weather), physical disasters (e.g.,fire, building collapse), human threats (intentional and unintentional), and any other identified physical security mechanisms, where deemed feasible and cost effective, to prevent or limit damage. Assistance in identifying physical security requirements can be obtained from AFI 31-209, The Installation and Resource Protection Program.

6.1.4.1. Entry Controls to the Computer Facility. All IS personnel shall control entry to the computer facility. Personnel shall be responsible for positive identification (by personal recognition) of persons attempting access to IS components. Personnel shall challenge any individual they cannot positively identify. If in doubt, personnel shall verify the status of the unknown individual. Status implies not only the need to access IS resources, but that the individual is authorized to perform the function for which access is requested and the function constitutes official business.

6.1.4.2. Resource Protection. IS personnel shall secure resources which process, store, or handle data within areas which provide adequate protection during and after duty hours. This requirement applies to all terminals, servers, routers and other equipment on the system. Removable storage media shall be stored in lockable containers when not in use.

6.1.4.3. Protection of Support Systems. Install surge protection or some form of electrical power conditioning on all electrical power sources serving IS resources.

6.1.4.3.1. Uninterruptable power supply (UPS) systems which will allow the primary resources to be gracefully brought down in the event of power failure shall be installed. Primary resources are those necessary for the system to continue operation such as servers and routers.

6.1.4.3.2. Personnel shall ensure fire extinguishers are readily accessible in all areas where IS resources are located.

6.1.5. Hardware. The CSO shall ensure hardware security controls meeting the requirements of AFI 33-209, The Resource Protection Program, are in place, documented, and implemented for each IS resource. The UCSO shall establish housekeeping procedures which prohibit eating, drinking, and smoking around IS assets and address their general exterior cleanliness and routine operator care.

6.1.6. Software. The use of the term software in this policy shall include operating system software and application software, to include database, spreadsheet, and word processing applications.

6.1.6.1. No person shall load or execute privately owned or “bulletin board” software on the IS. For personally written or locally developed software follow guidelines in AFSSI 5102 (AFI 33-202).

6.1.6.2. If a user needs to install public-domain software or shareware on an IS, the CSM shall approve installation on a case-by-case basis upon CSO certification that the software does not degrade/circumvent implemented security safeguards, and is safe for government use. In order to do this, the CSO shall check to see if the software is listed in the Evaluated Product List (EPL) or Air Force Assessed Product List (APL). The CSO may present an alternative method of certifying public-domain software or shareware for consideration as long as it provides a high degree of confidence that it will detect “Trojan horses” and other forms of malicious logic.

6.1.7. Contingency Planning:

6.1.7.1. Contingency Plans. The owner of the IS shall develop a standard contingency plan or Continuity of Operations Plan (COOP) to reduce the impact caused by unanticipated interruption of an IS operation. The contingency plan shall establish procedures to follow if a catastrophic event happens, how to reduce the impact from such events, and how to resume operations after the event. The plan shall address natural and system events. Such events or failures include: weather damage, water damage, loss of all or part of the system’s capabilities, inoperative components, defective storage media, maintenance problems, disruption to operations due to building evacuation, and complete or partial failure of security measures. AFM 10-401, USAF Operation Planning Process (FOUO); AFI 32-4001, Planning and Operations; and AFSSI 5019, Contingency Planning Guide (when published), provide contingency planning guidance. The CSM shall ensure individual installations can meet contingency processing requirements.

6.1.7.2. Backup and Recovery. The CSO shall maintain and make immediately available to IS personnel a roster of key people to be contacted during recovery operations. The CSO/SA shall ensure that backups or “save” actions of changed or updated files are made nightly. These backups may be retained on storage media, if available, for up to 1 week. At least weekly or when new software is installed and configured, the CSO/SA shall ensure a “save all” of the entire system is backed up to tape and the tape is stored in a secure location. The system shall automatically backup all critical files nightly. Critical files include security related and audit files as well as those designated as critical by operational personnel. All backups shall be stored in an off-site location. The vendor or contracted maintainer of unique or proprietary operating systems shall be required to have and make available on demand software or procedures for system/data recovery; viral protection, detection, and eradication (if appropriate); and system clearing/purging.

6.1.7.3. Emergency Response. The CSO/SA shall maintain a roster of key people to be contacted during emergency operations.

6.1.7.4. Exercising and Testing. The CSM and CSO shall review the contingency plan at least annually and conduct tests of the plan to ensure its adequacy. The CSO shall document the test.

6.1.8. Marking/Labeling. Personnel shall ensure that unclassified materials which require special marking and handling, such as For Official Use Only (FOUO) mandated by the Freedom of Information Act (FOIA), or Privacy Act, are marked in accordance with AFI 31-401, Information Security Management.

6.1.8.1. Automated Marking. The IS should automate as much marking of printed outputs as possible to relieve users from manually marking them. However, the CSO shall ensure users receive continual training and reminders that they, not the system, are responsible for the accuracy of these markings.

6.1.8.2. Marking Storage Media. Personnel shall use Air Force approved pressure sensitive labels to mark storage media at the highest level for which it was ever used.

6.1.8.3. Marking Peripheral Devices. Peripheral devices are not required to be marked.

6.1.9. Maintenance:

6.1.9.1. Maintenance on Hardware Devices. Maintainers of IS resources shall use only CSM approved maintenance procedures. A trained maintainer shall directly supervise all maintainers in training. System components shall be cleared of sensitive unclassified information using approved clearing procedures before releasing the equipment for maintenance.

6.1.9.2. Software Maintenance. The SA shall ensure periodic checks of operational software are performed by comparing the original application to that used on the operational system to detect any unauthorized changes. The UCSO shall ensure all original copies of software are write protected, inventoried, any copies and originals kept in a safe location.

6.1.10. Declassification/Destruction:

6.1.10.1. Declassification of Information. No special declassification procedures are necessary because classified information is not processed by ISs covered under this policy.

6.1.10.2. Destruction of Hardware Devices. Hardware devices which contain volatile and/or nonvolatile storage shall not be destroyed for security reasons.

6.1.10.3. Destruction of Storage Media. There is no requirement for the destruction of magnetic storage media containing sensitive unclassified information. Compact Discs are optical storage media that retain their highest sensitivity until destroyed. Destroy CDs in accordance with AFSSI 5020, Chapter 6.

6.1.10.4. Destruction of Output Products. FOUO and PA output data shall be destroyed in accordance with their respective Air Force directive publications by tearing, shredding, or incineration. FOUO and PA printed outputs shall not be commercially recycled unless such activity is approved by the cognizant authority for such actions. FOUO and PA printed output shall be locked up when not in use and destroyed when no longer needed. The DAA must approve the clearing procedures used. (Security police may authorize commercial recycling if the printed output products are shredded on site prior to removal from the installation.)

6.1.10.5. Inadvertent Classified Contamination. When classified information is discovered on the unclassified network, immediate action is required to minimize the unintentional exposure of classified information. The following is the sequence of actions required by the individual who discovers the classified information:

6.1.10.5.1 Individual discovering the classified information should immediately notify the Information Protection(IP) Branch (AFSOC/SCMS) and report the specifics of the incident. This should be done through your Computer System Security Officer (CSSO) if possible. **Do not delay** reporting the incident if the CSSO is not available. If you are unable to contact the Information Protection Branch notify the Network System Administrator of the specifics concerning the incident. If you are unable to contact anyone listed and/or the classified information was introduced into the Wing network you need to contact the Wing Information Protection Office and/or Wing Network System Administrator.

6.1.10.5.2 Individual discovering the incident should also notify their Security Manager who will then notify the Wing Information Security Program Manager (16th SFS/SPAI) and provide all requested information concerning the incident.

6.1.10.5.3 The Information Protection Branch should immediately notify and work with the Network System Administrator to identify the servers containing the classified information so they can be shut down and sanitized to preclude further propagation of the classified information. The Information Protection Office will also notify the CSSOs responsible for any unclassified workstations that may have had classified information placed on them for sanitization

6.1.11. Fraud, Waste, and Abuse (FWA). AFIs 15-1101 and 90-301, Air Force Fraud, Waste, and Abuse (FWA) Prevention and Detection, formalizes the Air Force commitment to prevent and eliminate fraud, waste, and abuse. It prescribes policy, establishes procedures, and provides guidance to make sure that resources allocated to the Air Force are applied effectively, to support national priorities. IS users and managers at all levels shall ensure fraud, waste, and abuse policies are supported. Additionally, no users shall violate copyright laws (specifically software and software documentation). Personnel must be aware of copyright restrictions placed on information system software.

6.1.12. Certification and Accreditation:

6.1.12.1. Security Certification Requirements. The owner of the IS will develop a security certification package in accordance with AFSSI 5024, Volume I, The Certification and Accreditation (C&A) Process and provide this certification package to the MAJCOM DAA. The following documents shall comprise the certification package:

6.1.12.1.1. Security Policy. This document shall describe the high level security requirements for ISs and the rules for protecting the information it contains, as well as the protection requirements that shall be met by external users and communications channels. It will be the basis for developing computer security plans, which may include a trusted facility manual (TFM) and Security Features Users Guide (SFUG).

6.1.12.1.2. Security Architecture. A graphically based security architecture shall describe security-related mechanisms incorporated within the IS. The security architecture shall illustrate the physical architecture of the system, layout of system components, and where the security mechanisms are located. Narrative descriptions of the security mechanisms will describe how security features operate, their interdependencies, and how they map to the Security Policy.

6.1.12.1.3. Security Plans. Security plans, mandate procedures and processes for end-using organizations to implement and use the system securely. Security plans, in combination with the security policy and security architecture, describe the required security environment for an IS.

6.1.12.1.4. System Description. A complete description, including hardware and software listings, of the standard IS.

6.1.12.1.5. Risk Analysis Report. The risk analysis shall provide an analysis of information containing the following activities and their associated stand alone documents. See AFSSI 5024, Volume II, The Certifying Official's Handbook for further information.

6.1.12.1.6. Sensitivity and Criticality Assessment. A sensitivity and Criticality Assessment shall document the importance to the operational mission of data processed by the IS and the extent to which its data must be protected from loss, unauthorized disclosure, or modification. See AFI 33-202 Air Force Computer Security Program, for further guidance on sensitivity and criticality.

6.1.12.1.7. Risk Assessment. The risk assessment includes a program level vulnerability assessment and threat assessment and shall document the IS vulnerabilities, threats common to most installations, likelihood of threat occurrence in a typical environment, degree of residual risk from matching threat vulnerability pairs, and the expected effectiveness of security measures.

6.1.12.1.8. Economic Assessment. The economic assessment shall document residual risks associated with the IS and possible countermeasures that could be applied to reduce those risks. The owner of the IS shall address approximate costs, manpower, schedule, and system performance impacts of proposed countermeasures.

6.1.12.1.9. Security Test and Evaluation (ST&E). The owner of the IS shall document a ST&E of the IS operating in the mandated security environment to determine if implemented security measures satisfy requirements.

6.1.12.1.10. IS Certification Letter. A certification letter signed by the CSO describes to what degree the IS meets security requirements, including any areas not meeting requirements, degree of risk associated with those areas, and procedural countermeasures implemented to mitigate those risks. This letter is the CSO's official certification that the IS, when used in accordance with the mandatory security environment, meets requirements and is suitable for it's intended mission.

6.1.12.1.11. Security Certification Requirements. The CSO shall review all system changes and updates for security impact, and update all security documentation as necessary. Upon a major change to the security environment, or after 3 years, the CSO will reaccomplish the risk analysis, recertify the system, and provide a new certification package to the designated DAA.

6.1.12.2. DAA Accreditation Requirements. A gaining operational DAA shall accredit the IS before it may be placed into operation supporting the mission. DAA accreditation, shall be official authorization for users to place the IS into operational use. The DAA shall base the accreditation decision on the IS CSOs certification that the level of residual risk in operating the system is sufficiently low to allow for its operational use, and the DAA's knowledge of the operational mission to be supported. If the operational system conforms to the operating environment as defined in the IS certification package, the DAA may elect to accredit the system with no further testing.

6.1.12.3. Accreditation Policy. The MAJCOM DAA may evaluate the wing level certification packages to determine if the IS meets applicable directives. If the MAJCOM DAA mandates additional requirements, or determines their users cannot meet the conditions of the mandatory security environment, the MAJCOM DAA will conduct additional risk analysis and ST&E to determine if the necessary degree of assurance can be achieved.

6.1.12.3.1. The MAJCOM DAA may develop a command-wide type accreditation package, including implementation plans to ensure end users install and use their systems in accordance with the mandatory security environment.

6.1.12.3.2. The MAJCOM type accreditation package will be provided to end user organizations, who must certify achievement of all mandatory requirements, and document this certification to the local DAA. If the local user mandates additional requirements, or determines the conditions of the mandatory security environment cannot be met, the using organization will conduct additional risk analysis and ST&E to determine if the necessary degree of assurance can be achieved.

6.2. Security Awareness, Training, and Education (SATE). Training shall promote proper and consistent application by users of basic IS security features and procedures to provide needed protection for information. It shall include training on procedures to report incidents and vulnerabilities under the Computer Security Technical Vulnerability Reporting Program (CSTVRP): AFI 33-225 shall be used for additional guidance. The CSO shall implement the SATE program in accordance with AFI 33-204, The Security Awareness, Training, and Education Program. Security training will be accomplished buy using the SAFE2 with compliance software and shall consist of initial security training, which shall be accomplished and documented for all personnel prior to their obtaining access, and annual security awareness refresher training. The CSM shall determine the level and content of the security training and it shall be consistent with AFI 33-204 and this policy. The CSO shall document training and both the trainer and trainee shall sign when it is performed. The CSO shall maintain the training documentation.

6.2.1. Depth of Training. Required depth of training shall depend on the security management position. For standard installations, depth of security awareness training requirements are:

6.2.1.1. CSO. The CSO is to be the IS' security expert. The CSO must have a complete understanding of the security requirements and the reporting of incidents and vulnerabilities (AFI 33-225).

6.2.1.2. UCSOs. UCSOs are responsible for the proper implementation of the system security program in their work area. Their training shall be primarily focused on the identification of practices dangerous to security and on the initial evaluation of suspected vulnerabilities or identified violations. The CSO shall be responsible for providing familiarization training to the UCSOs.

6.2.2. System Users. Depth of security awareness training for system users shall be primarily focused on the proper use of available system security features. UCSOs are responsible for providing users familiarization training.

7. Security Policy for Connecting to an IS:

7.1. Security Services Provided by the IS. Data entrusted to and received by the IS shall be protected at a C2 level of assurance from unauthorized disclosure. The IS shall provide for data integrity. Protocols that perform code or format conversion shall preserve integrity of entrusted data and control information. Personnel, physical, and administrative security mechanisms applied to the IS shall minimize risks of denial of service and unauthorized disclosure.

7.2. Security Procedures for Connecting to an IS. The DAA of systems or networks that desire connection to the IS must coordinate with IS' DAA throughout the subsequent procedures.

7.2.1. The DAA of systems or networks that desire connection must review the capabilities and limitations of the IS in terms of the security services provided and not provided, as identified in risk analysis and accreditation documentation. The IS' DAA shall provide risk analysis and accreditation information as necessary.

7.2.2. The DAA of a classified system interfacing with the IS for the purpose of importing sensitive unclassified information must provide assurance to the DAA that the interface is only one way and that classified data cannot corrupt the IS. The responsibility for ensuring the integrity of a one way interface rests with the DAA of the system with the higher classification. The one way interface of an IS to a classified system shall be mediated by at least a Class B1 device.

7.2.3. The DAA of systems or networks desiring connection shall provide the IS' DAA with a Memorandum of Agreement (MOA) which includes, as a minimum, data description and classification; user clearance levels; name of the DAA who shall resolve conflicts; intended recipients of transmitted data; and security mechanisms to be implemented before connecting to the IS. (Security mechanisms shall work two ways. They shall be present to protect connected data from disclosure or alteration to unauthorized users of the IS and they shall be in place to protect other IS users from unauthorized access via the connected network or system.) A sample MOA for user connection to the IS shall be part of the accreditation package presented to the DAA.

7.2.4. The IS' DAA shall approve the connectivity of systems or networks to or through that IS.

7.3. Connecting to the World Wide Web (Internet). For security reasons, network managers will maintain a database of all computer systems attached to their network that are capable of connecting to public access computer networks. The database will contain the user, user name, IP address, MAC address, location of workstation, port number, and machine type. Network managers will audit their networks on a periodic basis to ensure that only those users who have a valid need and have been adequately trained on security safeguards are given the capability to connect to the World Wide Web.

7.3.1. In addition, only publicly releasable information may be placed on the World Wide Web. Information that will be made public across the Web must be cleared through Public Affairs' channels. Public information includes any statements that suggest Air Force endorsement, policy, or identification of the source as an Air Force expert or spokesperson. The following types of information will <u>not</u> be placed on the World Wide Web or Internet:

7.3.1.1. Classified information.

7.3.1.2. Privacy Act information (AFI 37-132, Air Force Privacy Act Information).

7.3.1.3. For Official Use Only information and Freedom of Information Act-exempt information (AFI 37-131, Freedom of Information Act (FOIA)).

7.3.1.4. Unclassified information that requires special handling, such as Encrypt for Transmission Only (EFTO), limited distribution, and scientific and technical information.

7.3.2. The following statement must be placed on all AFSOC maintained bulletin boards and World Wide Web systems.

"USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."

8. Inability to Satisfy Requirements. There may be cases when implementing computer-based security hardware or software in an IS is not technically sound, violates the objective of economy by being prohibitively expensive, is time consuming, or will adversely impact the operational performance of the IS. Existence of such a case does not invalidate this policy, its objectives, or requirements. Rather, it challenges IS personnel to implement alternate security mechanisms which will satisfy intent of the policy until a more appropriate solution can be acquired. The selection of alternative security mechanism to compensate for an unrealistic solution will be considered temporary and requires periodic DAA review for its continued appropriateness.

DOUGLAS R. COLEMAND, Colonel, USAF
Director, Communications and Information